



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

| APPLICATION NO.                        | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|---------------------|------------------|
| 10/034,367                             | 12/27/2001  | Fabio R. Maino       | ANDIP004/425452     | 8712             |
| 22434                                  | 7590        | 08/19/2009           |                     |                  |
| Weaver Austin Villeneuve & Sampson LLP |             |                      | EXAMINER            |                  |
| P.O. BOX 70250                         |             |                      | TESLOVICH, TAMARA   |                  |
| OAKLAND, CA 94612-0250                 |             |                      |                     |                  |
|  |             | ART UNIT             | PAPER NUMBER        |                  |
|  |             | 2437                 |                     |                  |
|  |             | MAIL DATE            | DELIVERY MODE       |                  |
|  |             | 08/19/2009           | PAPER               |                  |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/034,367

**Applicant(s)**

MAINO ET AL.

**Examiner**

Tamara Teslovich

**Art Unit**

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 May 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-48 is/are pending in the application.
- 4a) Of the above claim(s) 1-25 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 26-48 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-946)
- 3) ☐ Information Disclosure Statement(s) (PTO/SG/US)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

This Office Action is in response to Applicant's Remarks and Amendments filed May 21, 2009.

Claims 1-25 remain withdrawn.

Claims 49-50 are cancelled.

Claims 26-48 are pending and herein considered.

### **Response to Arguments**

Applicant's arguments filed May 21, 2009 have been fully considered but they are not persuasive.

The Examiner respectfully disagrees with Applicant's first set of arguments directed towards Hawe and Hagerman's alleged failure to teach or suggest a security enable indicator. The Examiner would like to begin by drawing attention to the Summary of the Invention of the Hawe reference, particularly column 6 lines 9-20 wherein Hawe discloses a method and related apparatus for including a special cryptographic preamble at the beginning of each packet. Hawe goes on in lines 36-54 of that same column to describe how that cryptographic preamble includes an offset field to indicate the location of data to be cryptographically processed as well as a mode field indicating the type of cryptographic processing to be performed. A number of available modes exist and the system determines whether or not a particular packet

requires cryptographic processing by examining the contents of the cryptographic preamble. It is this preamble that the Examiner has equated with Applicant's "security enable indicator" because it allows a system to determine whether a particular packet has been encrypted and how so that the necessary actions may be taken thereupon.

The Examiner respectfully disagrees with Applicant's next set of remarks concerning Hawe and Hagerman's alleged failure to teach or suggest a first frame having a security enable indicator and a second frame having a security control indicator. As noted above, the Examiner has equated Applicant's security enable indicators with Hawe's cryptographic preambles insofar as they exist at the beginning of each packet in order to avoid having to parse each information packet in detail and account for differences in protocol and packet formats (Hawe col.6 lines 9-20).

The Examiner respectfully disagrees with Applicant's next set of remarks concerning Hawe and Hagerman's alleged failure to teach or suggest wherein the first frame is associated with a fabric login or a port login message. While it is true that the primary reference Hawe fails to specifically teach wherein the first frame is associated with a fabric login or port login message, the Examiner has relied upon Hagerman in conjunction with Hawe because Hawe not only teaches a secure fibre channel communication network, but also teaches frames associated with fabric login or port login messages (col.6 lines 1-14 "switched fabric" and "Fibre Channel arbitrated Loop Technology") and the transmission of acknowledgements to a second network entity that the first network entity supports security, the acknowledgement including algorithm information (col.3 lines 34-37; col.5 lines 15-41) and security association identifiers

associated with frames which correspond to an entry in a security database (col.3 lines 43-47; col.7 lines 11-34).

It is based upon the above made arguments in view of the prosecution history in its entirety that the Examiner maintains her 35 U.S.C. 103 rejection of claims 26-48 as unpatentable over United States Patent No. 5,070,528 to Hawe et al. and further in view of US Patent No. 6,973,568 B2 to Hagerman, included below.

**Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 26-48** are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 5,070,528 to Hawe et al. and further in view of US Patent No. 6,973,568 B2 to Hagerman.

As per **claim 26**, Hawe teaches a method for processing frames in a fibre channel network having a first network entity and a second network entity, the method comprising:

receiving a first frame at the first network entity from the second network entity in the fibre channel network and identifying a security enable parameter in the first frame (col.8 lines 6-23; col.10 lines 45-60);

receiving a second frame at the first network entity from the second network entity (col.8 lines 24-51);

identifying a security control indicator in the second frame from the second network entity, wherein the security control indicator is used to determine if the second frame is encrypted (col.6 lines 36-54);

decrypting a first portion of the second frame (col.16 lines 1-14).

Hawe fails to teach wherein the first frame is associated with a fabric login or port login message, transmitting an acknowledgement to the second network entity that the first network entity supports security, the acknowledgement including algorithm information and determining that a security association identifier associated with the frame corresponds to an entry in a security database and decrypting the first portion of the frame by using algorithm information contained in the entry in the security database. Hawe also fails to provide for authentication of any type.

Hagerman teaches a secure fibre channel communication network wherein a first frame is associated with a fabric login or port login message (col.6 lines 6-13), transmitting an acknowledgement to the second network entity that the first network entity supports security, the acknowledgement including algorithm information (col.3 lines 34-47; col.5 lines 15-41) and utilizing security association identifiers associated with frames which correspond to an entry in a security database (col.3 lines 43-47; col.7

lines 11-34) and decrypting the first portion of the frame by using algorithm information contained in the entry in the security database (col.7 lines 11-34). Hagerman goes on to teach the use of authentication within his system to provide for additional security (Abstract, col.3 lines 23-42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Hawe the login messages, acknowledgements, algorithm information, authentication, security database, and decryption utilizing the security database as described in Hagerman to provide increased levels of security and overall scalability.

As per **claim 27**, the combined method of Hawe and Hagerman teaches wherein the entry in the security database was created after a fibre channel network authentication sequence between the first and second network entities (Hagerman col.7 lines 1-10).

As per **claim 28**, the combined method of Hawe and Hagerman teaches wherein the first portion is decrypted using a key contained in the entry in the security database (Hagerman col.3 lines 43-53).

As per **claim 29**, the combined method of Hawe and Hagerman teaches wherein the first portion is encrypted using DES, 3DES or AES (Hagerman col.7 lines 1-10).

As per **claim 30**, the combined method of Hawe and Hagerman teaches recognizing that a second portion of the second frame supports authentication; using algorithm information contained in the entry in the security database to authenticate the second portion of the second frame (Hagerman col.5 lines 15-41).

As per **claim 31**, the combined method of Hawe and Hagerman teaches wherein the second portion is authenticated using MD5 or SHA1 (Hagerman col.3 lines 34-42; col.7 lines 35-44).

As per **claim 32**, the combined method of Hawe and Hagerman teaches wherein the authentication sequence is a fibre channel login sequence between the first and second network entities (Hagerman col.3 lines 34-47).

As per **claim 33**, the combined method of Hawe and Hagerman teaches wherein the login sequence is a PLOGI or FLOGI sequence (Hagerman col.6 lines 6-13).

As per **claim 34**, the combined method of Hawe and Hagerman teaches wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence (Hagerman col.1 lines 28-40).



As per **claim 35**, the combined method of Hawe and Hagerman teaches wherein the first and second network entities are domain controllers and the authentication sequence is a SW-TL sequence (Hagerman col.6 lines 6-14).

As per **claim 36**, Hawe teaches a method for transmitting encrypted frames in a fibre channel network having a first network entity and a second network entity, the method comprising: transmitting a first fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity (col.8 lines 24-51), the first fibre channel frame including a security enable indicator (col.8 lines 6-23; col.10 lines 45-60); identifying a second fibre channel frame having a source corresponding to the first network entity and a destination corresponding to the second network entity (col.8 lines 24-51); providing a security control indicator in the second fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted and authenticated (col.6 lines 36-54); transmitting the second fibre channel frame to the second network entity (col.8 lines 24-51).

Hawe fails to teach wherein the first fibre channel frame is associated with a fabric login or a port login message, receiving an acknowledgement from the second network entity indicating that the second network entity supports security, inserting key and algorithm information from the second network entity into a security database and determining if a security association identifier associated with the frame corresponds to an entry in a security database and encrypting the first portion of the frame by using

algorithm information contained in the entry in the security database. Hawe also fails to provide for authentication of any type.

Hagerman teaches a secure fibre channel communication network wherein the first fibre channel frame is associated with a fabric login or a port login message (col.6 lines 6-13), receiving an acknowledgement from the second network entity indicating that the second network entity supports security (col.3 lines 34-47; col.5 lines 15-41), inserting key and algorithm information from the second network entity into a security database and utilizing security association identifiers associated with frames which correspond to an entry in a security database (col.3 lines 43-47; col.7 lines 11-34) and encrypting the first portion of the frame by using algorithm information contained in the entry in the security database (col.7 lines 11-34). Hagerman goes on to teach the use of authentication within his system to provide for additional security (Abstract, col.3 lines 23-42).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Hawe the login message, acknowledgements, authentication, security database with key and algorithm information, and encryption utilizing the security database as described in Hagerman to provide increased levels of security and overall scalability.

As per **claim 37**, the combined method of Hawe and Hagerman teaches wherein the entry in the security database was created after a fibre channel network

authentication sequence between the first and second network entities (Hagerman col.7 lines 1-10).

As per **claim 38**, the combined method of Hawe and Hagerman teaches wherein the payload is encapsulated using the Authentication Header protocol or the Encapsulating Security Payload protocol (Hagerman col.7 lines 1-10).

As per **claim 39**, the combined method of Hawe and Hagerman teaches adding security information to the header of the second fibre channel frame (Hagerman col.3 lines 23-33).

As per **claim 40**, the combined method of Hawe and Hagerman teaches wherein a first portion of the fibre channel frame is encrypted using DES, 3DES, or AES (Hagerman col.7 lines 1-10).

As per **claim 41**, the combined method of Hawe and Hagerman teaches wherein parameters in the header are normalized prior to encrypting the first portion of the second fibre channel frame (Hagerman col.3 lines 48-53).

As per **claim 42**, the combined method of Hawe and Hagerman teaches wherein the payload is padded prior to encrypting the first portion of the fibre channel frame (Hagerman col.5 lines 3-25).

As per **claim 43**, Hagerman teaches computing authentication data using key and algorithm information as well as a second portion of the second fibre channel frame (Hagerman col.5 lines 15-25).

As per **claim 44**, the combined method of Hawe and Hagerman teaches wherein authentication data is computed using MD5 or SHA1 (Hagerman col.3 lines 34-42; col.7 lines 35-44).

As per **claim 45**, the combined method of Hawe and Hagerman teaches wherein the authentication sequence is a fibre channel login sequence between the first and second network entities (Hagerman col.3 lines 34-47).

As per **claim 46**, the combined method of Hawe and Hagerman teaches wherein the login sequence is a PLOGI or FLOGI sequence (Hagerman col.6 lines 6-13).

As per **claim 47**, the combined method of Hawe and Hagerman teaches wherein the first and second network entities are domain controllers and the authentication sequence is a FC-CT sequence or an SW-ILS message (Hagerman col.1 lines 28-40; col.6 lines 6-14).

**Claim 48** corresponds to an apparatus employing the method described in claim 36 and is rejected accordingly.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571)272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/  
Examiner, Art Unit 2437

/Matthew B Smithers/  
Primary Examiner, Art Unit 2437